DEPARTMI

Privacy Act of 1974; System of Records

AGENCY: Veterans Affairs Central Office (VACO) and Office of Operations, Security, and Preparedness, Department of Veterans Affairs (VA).

ACTION: Notice of a modified system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, notice is hereby given that the Department of Veterans Affairs (VA) is modifying an existing system of records entitled, ‘‘Department of Veterans Affairs Personnel Security File System-VA (VAPSFS)’’ 145VA005Q3). The modification to the existing system of records addresses modernized system processes and updated routine uses. This system of records supports the Department in conducting end-to-end personnel security, fitness, suitability, and credentialing processes. This system of records contains records related to employee and contractor vetting as well as investigative, administrative, adjudicative, and/or determination information for decisions concerning whether an individual is suitable or fit for Government employment or eligible to access classified national security information.

DATES: Comments on this modified system of records must be received no later than 30 days after date of publication in the Federal Register. If no public comment is received during the period allowed for comment or unless otherwise published in the Federal Register by VA, the modified system of records will become effective a minimum of 30 days after date of publication in the Federal Register. If VA receives public comments, VA shall review the comments to determine whether any changes to the notice are necessary.

ADDRESSES: Comments may be submitted through https://www.regulations.gov or mailed to VA Privacy Service, 810 Vermont Avenue, NW (005R1A), Washington, DC 20420. Comments should indicate that they are submitted in response to “Department

of Veterans Affairs Personnel Security File System (VAPSFS)-VA'' 145VA005Q3)". Comments received will be available at https://www.regulations.gov for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT: Trish Moore, Director, Department of Veterans Affairs Personnel Security and Credential Management (PSCM) Program Manager, VA Central Office (VACO), 810 Vermont Avenue, Room C-6, Washington, DC 20420, (202) 461-0496/5240 (These are not toll-free numbers).

SUPPLEMENTARY INFORMATION: The VA Personnel Security File System (VAPSFS) (also known as the "Veterans Affairs Centralized Adjudication Background Investigation System (VA-CABS)") is an enterprise-wide, standardized, and integrated case management system for adjudication, background investigation, and reinvestigation processes. VA-CABS will serve as the department's system of records for adjudication and investigation-related data.

This system supports the Department in conducting end-to-end personnel security, fitness, suitability, and credentialing processes. This system of records contains records related to employee and contractor vetting as well as investigative, administrative, adjudicative, and/or determination information for decisions concerning whether an individual is suitable or fit for Government employment or eligible to access classified national security information.

VA CABS maintains information on security clearance access, personnel security eligibility, suitability for Government employment, fitness to perform work for or on behalf of the U.S. Government as a contractor. It also provides an all-inclusive medium to document personnel security adjudicative actions within the agency, allowing users to provide investigation and adjudication updates to security managers and other security officials.

All users of VA-CABS must be appropriately screened, investigated, and granted

access based on the user's specific functions, security eligibility, and access level.

VA-CABS will be used to ensure VA is upholding the highest standards of integrity, loyalty, conduct, and security among its employees and contract personnel.

It will also help streamline the vetting process by utilizing a single system for all phases of vetting operations to include adjudication, continuous evaluation/continuous vetting, and case management, while maintaining compliance with all applicable legal, regulatory and policy authorities.

Signing Authority

The Senior Agency Official for Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs. Kurt D. DelBene, Assistant Secretary for Information and Technology and Chief Information Officer, approved this document on May 25, 2022 for publication.

Dated: June 28, 2022

Amy L. Rose,

Program Analyst,

VA Privacy Service,

Office of Information Security,

Office of Information and Technology,

Department of Veterans Affairs.

SYSTEM NAME AND NUMBER: Department of Veterans Affairs Personnel Security File System-VA (VAPSFS) — (145VA005Q3)

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: Electronic records are kept at the VA Data Centers at Falling Waters, WV; Hines, IL; Austin Automation Center, Austin, TX; and at the SIC, Little Rock, AR.

SYSTEM MANAGER(S): Officials responsible for policies and procedures: Trish Moore, Department of Veterans Affairs Personnel Security and Credential Management (PSCM) Director, VA Central Office (VACO), 810 Vermont Avenue, Room C- 6, Washington, DC 20420, (202) 461-0496/5240. The Authorizing Official for VA-CABS is Daniel McCune, Department of Veterans Affairs Office of Information and Technology, Enterprise Program Management Office Executive Director, 810 Vermont Avenue, Room 340, Washington, DC 20420, 202-632-7390 (these are not toll-free numbers).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Executive Orders 9397, 10450, 10865, 12333, and 12356; 5 U.S.C 3301 and 9101; 42 U.S.C 2165 and 2201; 50 U.S.C 781 to 887; 5 C.F.R 5, 732, and 736; and Homeland Security Presidential Directive 12.

PURPOSE(S) OF THE SYSTEM: The records in this system are used to provide investigative and related administrative, adjudicative, and other information necessary to determine whether an individual is suitable or fit for Government employment; eligible for physical access to VA controlled facilities and information systems; eligible to hold sensitive positions (including but not limited to eligibility for access to classified information); fit to perform work for or on behalf of the U.S. Government as a contractor; qualified to perform contractor services for the U.S. Government; or loyal to the United States; while maintaining compliance with applicable legal, regulatory and policy authorities.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: (1) Current and former government employees, applicants, volunteers, health professions trainees, consultants, experts, and contractor personnel working for or on behalf of the VA; (2) personnel who are appealing a denial or a revocation of a Veterans Affairs-issued security clearance; (3) employees and contractor personnel who have applied for the HSPD–12 Personal Identity Verification (PIV) Card; (5) individuals who are not Veterans Affairs employees, but who are or were involved in Veterans Affairs programs under a cooperative assignment or under a similar agreement. As part of the on-boarding process, VA Subjects undergo a Special Agency Check (SAC) (fingerprint) and a background investigation based on their position sensitivity and risk designation.

CATEGORIES OF RECORDS IN THE SYSTEM: Applicable records containing the following information from one or more of the categories within background investigations relating to personnel investigations conducted by the Defense Counterintelligence and Security Agency (DCSA) and other Federal agencies and departments on a pre-placement and post-placement basis to make suitability, fitness, and HSPD–12 PIV determinations and for granting security clearances.

This system maintains information collected as part of the investigative vetting process. This information may include the individual's personally identifiable information; residential, educational, employment, and mental health history; financial details, and criminal and disciplinary histories; to include:

(1) An individual's name, former names and aliases; date and place of birth; social security number (SSN); height; weight; hair and eye color; gender; mother's maiden name; current and former home addresses to include names and addresses of neighbors and references, phone numbers, and email addresses; employment history to include names of supervisors and colleagues; military record information; selective service registration record; education and degrees earned; names of associates and

references with their contact information; citizenship; passport information; criminal history; civil court actions; prior security clearance and investigative information; mental health history; records related to drug and/or alcohol use; credit reports; the name, date and place of birth, SSN, and citizenship information for spouse or cohabitant; the name and marriage information for current and former spouse(s); the citizenship, name, date and place of birth, and address for relatives; information on foreign contacts and activities; association records; information on loyalty to the United States; publicly available social media information; and other agency reports furnished to VA in connection with the background investigation process, and other information developed from the above;

(2) Position designation/risk/sensitivity; status of current adjudicative action; status of security clearance eligibility and/or access, suitability, fitness, or HSPD–12 PIV determinations; and investigative records related to initial vetting, reinvestigation, continuous evaluation, and/or continuous vetting;

(3) Summaries of personal and third-party interviews conducted during the background investigation;

(4) Signed Classified Information Non-Disclosure Agreement (SF 312), and related supplemental documents for those persons issued a security clearance;

(5) An automated data system reflecting identification data on incumbents and former employees, disclosure and authorization forms, and record of investigations, level and date of security clearance, if any, as well as status of investigations;

(6) Records pertaining to suspensions or an appeal of a denial or a revocation of a VA-issued security clearance;

(7) Records pertaining to the personal identification verification process mandated by HSPD–12 and the issuance, denial or revocation of a PIV card; and

(8) Records of personnel background investigations conducted by other Federal agencies.

RECORD SOURCE CATEGORIES: Records are obtained from individual employees, applicants, detailees, consultants, experts and contractors (including the results of in-person interviews) whose files are on record as authorized by those concerned; investigative reports from federal investigative agencies; criminal or civil investigations; continuous evaluation records; police and credit record checks; personnel records; educational records and instructors; current and former employers; coworkers, neighbors, family members, acquaintances; and authorized security representatives.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

1. Congress: VA may disclose information to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

2. Data breach response and remediation, for VA: VA may disclose information to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the system of records,· (2) VA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, VA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with VA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

3. Data breach response and remediation, for another Federal agency: VA may disclose information to another Federal agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing,

minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

4. Law Enforcement: VA may disclose information that, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, to a Federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law. The disclosure of the names and addresses of veterans and their dependents from VA records under this routine use must also comply with the provisions of 38 U.S.C. 5701.

5. DoJ for Litigation or Administrative Proceeding: VA may disclose information to the Department of Justice (DoJ), or in a proceeding before a court, adjudicative body, or other administrative body before which VA is authorized to appear, when:

(a) VA or any component thereof;

(b) Any VA employee in his or her official capacity;

(c) Any VA employee in his or her individual capacity where DoJ has agreed to represent the employee; or

(d) The United States, where VA determines that litigation is likely to affect the agency or any of its components,

is a party to such proceedings or has an interest in such proceedings, and VA determines that use of such records is relevant and necessary to the proceedings.

6. Contractors: VA may disclose information to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for VA, when reasonably necessary to accomplish an agency function related to the records.

7. OPM: VA may disclose information to the Office of Personnel Management (OPM) in connection with the application or effect of civil service laws, rules, regulations, or OPM guidelines in particular situations.

8. EEOC: VA may disclose information to the Equal Employment Opportunity Commission (EEOC) in connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or other functions of the Commission as authorized by law.

9. FLRA: VA may disclose information to the Federal Labor Relations Authority (FLRA) in connection with: the investigation and resolution of allegations of unfair labor practices, the resolution of exceptions to arbitration awards when a question of material fact is raised; matters before the Federal Service Impasses Panel; and the investigation of representation petitions and the conduct or supervision of representation elections.

10. MSPB: VA may disclose information to the Merit Systems Protection Board (MSPB) and the Office of the Special Counsel in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigation of alleged or possible prohibited personnel practices, and such other functions promulgated in 5 U.S.C. 1205 and 1206, or as authorized by law.

11. NARA: VA may disclose information to NARA in records management inspections conducted under 44 U.S.C. 2904 and 2906, or other functions authorized by laws and policies governing NARA operations and VA records management responsibilities.

13. Federal Agencies, Courts, Litigants, for Litigation or Administrative Proceedings: To another federal agency, court, or party in litigation before a court or in an administrative proceeding conducted by a Federal agency, when the government is a party to the judicial or administrative proceeding.

14. Governmental Agencies, Health Organizations, for Claimants' Benefits: To Federal, state, and local government agencies and national health organizations as reasonably

necessary to assist in the development of programs that will be beneficial to claimants, to protect their rights under law, and assure that they are receiving all benefits to which they are entitled.

15. Governmental Agencies, for VA Hiring, Security Clearance, Contract, License, Grant: To a Federal, state, local, or other governmental agency maintaining civil or criminal violation records, or other pertinent information, such as employment history, background investigations, or personal or educational background, to obtain information relevant to VA's hiring, transfer, or retention of an employee, issuance of a security clearance, letting of a contract, or issuance of a license, grant, or other benefit. The disclosure of the names and addresses of veterans and their dependents from VA records under this routine use must also comply with the provisions of 38 U.S.C. 5701.

16. Federal Agencies, for Employment: To a Federal agency, except the United States Postal Service, or to the District of Columbia government, in response to its request, in connection with that agency's decision on the hiring, transfer, or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit by that agency.

17. State or Local Agencies, for Employment: To a state, local, or other governmental agency, upon its official request, as relevant and necessary to that agency's decision on the hiring, transfer, or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit by that agency. The disclosure of the names and addresses of veterans and their dependents from VA records under this routine use must also comply with the provisions of 38 U.S.C. 5701.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records in this system are stored electronically.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by name, social security number, date of birth, place of birth, Defense

Counterintelligence and Security Agency [Investigative Service Provider] investigation number, adjudicative case identification number or some combination thereof.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States. Records on government employees and contractor personnel are retained for 5 years after the employee or contractor relationship ends, but longer retention is authorized if required for business use in accordance with General Records Schedule 5.6, item 181. The records on applicants not selected and separated employees are destroyed or sent to the Federal Records Center in accordance with General Records Schedule 5.6, item 180. Investigative reports are maintained in OPM Central-9 (81 FR 70191).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Electronic records are maintained in a secure, SSOi protected electronic system that utilizes security hardware and software to include: Encryption, multiple firewalls, active intruder detection, and role-based access controls.

Safeguarding VA Subjects' adjudicative and background investigation information is of the utmost importance. Information collected or used in the adjudicative process will be used and disseminated under very strict controls. Permission shall be obtained from DCSA to release any DCSA or other agency investigative material. Reports, records, and files pertaining to adjudicative matters must be maintained in confidence and disseminated only to authorized officials in the VA having a clear, official need to review the material.

RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above. A request for access to records must contain the requester’s full name, address, telephone number, be signed by the requester, and

describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

CONTESTING RECORD PROCEDURES: Individuals seeking to contest or amend records in this system pertaining to them should contact the system manager in writing as indicated above. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

NOTIFICATION PROCEDURES: Generalized notice is provided by the publication of this notice. For specific notice, see Record Access Procedure, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Upon publication of a final rule in the Federal Register, this system of records will be exempt in accordance with 5 U.S.C. 552a(k)(5). Information will be withheld to the extent it identifies witnesses promised confidentiality as a condition of providing information during the course of the background investigation.

HISTORY: 73 FR 15852 (March 25, 2008).

[FR Doc. 2022-14118 Filed: 6/30/2022 8:45 am; Publication Date: 7/1/2022]